# Method And Apparatus For Securely Transferring Data

Field of the Invention

The present invention relates to a method and system for securely transferring data.

5

Background of the Invention

With the wide spread use of the Internet commercial transactions over the Internet have become commonplace. However, unlike commercial transactions that are conducted face-to-face, transactions over the Internet typically involve the exchange of private and confidential information, for example providing access to a party's bank account details, credit card details and home address.

Accordingly, many individuals still have concerns over confidentiality; as a result the full potential of the Internet is still not being utilized.

It is desirable to improve this situation.

Embodiments of the present invention to be described hereinafter make use of a cryptographic technology known as identifier-based encryption. Accordingly, a brief description will now be given of this type of encryption.

Identifier-Based Encryption (IBE) is an emerging cryptographic schema. In this schema (see Figure 1 of the accompanying drawings), a data provider 10 encrypts payload data 13 using both an encryption key string 14, and public data 15 provided by a trusted authority12. This public data 15 is derived by the trusted authority 12 using private data 17 and a one-way function 18. The data provider 10 then provides the encrypted payload data <13> to a recipient 11 who decrypts it, or has it decrypted, using a decryption key computed by the trusted authority 12 based on the encryption key string and its own private data.

30

A feature of identifier-based encryption is that because the decryption key is generated from the encryption key string, its generation can be postponed until needed for decryption.

5    Another feature of identifier-based encryption is that the encryption key string is cryptographically unconstrained and can be any kind of string, that is, any ordered series of bits whether derived from a character string, a serialized image bit map, a digitized sound signal, or any other data source. The string may be made up of more than one component and may be formed by data already subject to upstream

10   processing. In order to avoid cryptographic attacks based on judicious selection of a key string to reveal information about the encryption process, as part of the encryption process the encryption key string is passed through a one-way function (typically some sort of hash function) thereby making it impossible to choose a cryptographically-prejudicial encryption key string. In applications where defence against such attacks is

15   not important, it would be possible to omit this processing of the string.

Frequently, the encryption key string serves to "identify" the intended message recipient and this has given rise to the use of the label "identifier-based" or "identity-based" generally for cryptographic methods of the type under discussion. However,

20   depending on the application to which such a cryptographic method is put, the string may serve a different purpose to that of identifying the intended recipient and, indeed, may be an arbitrary string having no other purpose than to form the basis of the cryptographic processes. Accordingly, the use of the term "identifier-based" or "IBE" herein in relation to cryptographic methods and systems is to be understood simply as

25   implying that the methods and systems are based on the use of a cryptographically unconstrained string whether or not the string serves to identify the intended recipient. Generally, in the present specification, the term "encryption key string" or "EKS" is used rather than "identity string" or "identifier string".

30   A number of IBE algorithms are known and Figure 2 indicates, for three such algorithms, the following features, namely:

- the form of the encryption parameters used, that is, the encryption key string and the public data of the trusted authority (TA);

- the conversion process applied to the encryption key string to prevent attacks based on judicious selection of this string;

5    - the primary encryption computation effected;

- the form of the encrypted output.

The three prior art IBE algorithms to which Figure 2 relates are:

**Quadratic Residuosity (QR) method** as described in the paper: C. Cocks, "An identity based encryption scheme based on quadratic residues", Proceedings of the

10    $8^{th}$ IMA International Conference on Cryptography and Coding, LNCS 2260, pp 360-363, Springer-Verlag, 2001. A brief description of this form of IBE is given hereinafter.

- **Bilinear Mappings** $p$ using, for example, a Tate pairing $t$ or Weil pairing $\hat{e}$. Thus, for the Weil pairing:

15       $\hat{e}: G_1 \times G_1 \longrightarrow G_2$

where $G_1$ and $G_2$ denote two algebraic groups of prime order $q$ and $G_2$ is a subgroup of a multiplicative group of a finite field. The Tate pairing can be similarly expressed though it is possible for it to be of asymmetric form:

$t: G_1 \times G_0 \longrightarrow G_2$

20    where $G_0$ is a further algebraic group the elements of which are not restricted to being of order q. Generally, the elements of the groups $G_0$ and $G_1$ are points on an elliptic curve though this is not necessarily the case. A description of this form of IBE method, using Weil pairings is given in the paper: D. Boneh, M. Franklin – "Identity-based Encryption from the Weil Pairing" in *Advances in Cryptology -*

25    *CRYPTO 2001*, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

- **RSA-Based methods** The RSA public key cryptographic method is well known and in its basic form is a two-party method in which a first party generates a public/private key pair and a second party uses the first party's public key to encrypt messages for sending to the first party, the latter then using its private key

30    to decrypt the messages. A variant of the basic RSA method, known as "mediated RSA", requires the involvement of a security mediator in order for a message

recipient to be able to decrypt an encrypted message. An IBE method based on mediated RSA is described in the paper "Identity based encryption using mediated RSA", D. Boneh, X. Ding and G. Tsudik, 3rd Workshop on Information Security Application, Jeju Island, Korea, Aug, 2002.

5

A more detailed description of the QR method is given below with reference to the entities depicted in Figure 1 and using the same notation as given for this method in Figure 2. In the QR method, the trusted authority's public data 15 comprises a value $N$ that is a product of two random prime numbers $p$ and $q$, where the values of $p$ and $q$

10   are the private data 17 of the trusted authority 12. The values of $p$ and $q$ should ideally be in the range of $2^{511}$ and $2^{512}$ and should both satisfy the equation: $p, q \equiv 3 \bmod 4$. However, $p$ and $q$ must not have the same value. Also provided is a hash function # which when applied to a string returns a value in the range 0 to $N$-1.

15   Each bit of the user's payload data 13 is then encrypted as follows:
- The data provider 10 generates random numbers $t_+$ (where $t_+$ is an integer in the range [0, $2^N$]) until a value of $t_+$ is found that satisfies the equation $jacobi(t_+, N)$=m', where m' has a value of –1 or 1 depending on whether the corresponding bit of the user's data is 0 or 1 respectively. (As is well known, the

20   *jacobi* function is such that where $x^2 \equiv \# \bmod N$ the jacobi (#, $N$) = -1 if x does not exist, and = 1 if x does exist). The data provider 10 then computes the value:

$$s_+ \equiv (t_+ + K/t_+) \bmod N$$

where: $s_+$ corresponds to the encrypted value of the bit m' concerned, and

$K$ = #(encryption key string)

25

- Since $K$ may be non-square, the data provider additionally generates additional random numbers $t_-$ (integers in the range [0, $2^N$)) until one is found that satisfies the equation $jacobi(t_-, N)$= m'. The data provider 10 then computes the value:

$$s_- \equiv (t_- - K/t_-) \bmod N$$

as the encrypted value of the bit m concerned.

The encrypted values $s_+$ and $s_-$ for each bit *m'* of the user's data are then made available to the intended recipient 11, for example via e-mail or by being placed in a electronic public area; the identity of the trusted authority 12 and the encryption key string 14 will generally also be made available in the same way.

The encryption key string 14 is passed to the trusted authority 12 by any suitable means; for example, the recipient 11 may pass it to the trusted authority or some other route is used - indeed, the trusted authority may have initially provided the encryption key string. The trusted authority 12 determines the associated private key *B* by solving the equation :

$$B^2 \equiv K \bmod N \qquad \text{("positive" solution)}$$

If a value of B does not exist, then there is a value of B that is satisfied by the equation:

$$B^2 \equiv - K \bmod N \qquad \text{("negative" solution)}$$

As N is a product of two prime numbers p, q it would be extremely difficult for any one to calculate the decryption key *B* with only knowledge of the encryption key string and *N*. However, as the trusted authority 12 has knowledge of *p* and *q* (i.e. two prime numbers) it is relatively straightforward for the trusted authority 12 to calculate *B*.

Any change to the encryption key string 14 will result in a decryption key 16 that will not decrypt the payload data 13 correctly. Therefore, the intended recipient 11 cannot alter the encryption key string before supplying it to the trusted authority 12.

The trusted authority 12 sends the decryption key to the data recipient 11 along with an indication of whether this is the "positive" or "negative" solution for *B*.

If the "positive" solution for the decryption key has been provided, the recipient 11 can now recover each bit *m'* of the payload data 13 using:

$$m' = jacobi(s_+ + 2B, N)$$

If the "negative" solution for the decryption key *B* has been provided, the recipient 11 recovers each bit *m'* using:

$$m' = jacobi(s_- + 2B, N)$$

## Summary of the Invention

In accordance with a first aspect of the present invention there is provided a method of securely transferring first and second data from a user to first and second parties respectively, wherein:

- the user encrypts the first data using a first encryption key associated with the first party, and then encrypts the second data using, as encryption parameters, both public data of said first party and third data comprising the encrypted first data;

- the third data is provided to the first party and the encrypted second data is provided to the second party;

- the first party uses a first decryption key to decrypt the encrypted first data, as provided to the first party in said third data, whereby to recover the first data; the first party also using the third data, along with private data related to said public data, to generate a second decryption key;

- the second decryption key is provided to the second party which uses it to decrypt the encrypted second data.

Typically, the first data comprises a message with interpretable content. For example, the message may comprises an instruction to the first party to carry out a specific action, the first party interpreting the recovered first data and carrying out said specific action. The message may alternatively or additionally comprise a condition to be satisfied before the second decryption key is provided to the second party, the first party interpreting the recovered first data and ensuring that said condition is satisfied

before it generates said second decryption key and/or provides that key to the second party.

Conveniently, the user sends the encrypted second data, together with the third data, to the second party; the second party then being responsible for providing the third data to the first party.

In accordance with a second aspect of the present invention there is provided a computer system comprising first, second and third computing entities, wherein:

- the first computing entity comprises a first arrangement for encrypting a first data set using a first encryption key associated with a third party; a second arrangement for encrypting a second data set using, as encryption parameters, both public data of said third party and a third data set comprising the encrypted first data set; and a third arrangement for outputting the encrypted second data set for provision to the second computing entity and for outputting the third data set for provision to the third computing entity; and

- the third computing entity is associated with said third party and is arranged to use a first decryption key to decrypt the encrypted first data as provided to the third computing entity in said third data set whereby to recover the first data set; the third computing entity being further arranged to generate, using the third data set and private data related to said public data, a second decryption key for enabling the second computing entity to decrypt the encrypted second data set.

In accordance with a third aspect of the present invention there is provided apparatus comprising:

- first means for forming a first data set comprising a message intended for a trusted authority;
- second means for encrypting the first data set using an encryption key associated with the trusted authority;

- third means for encrypting a second data set using, as encryption parameters, both public data of the trusted authority and a third data set comprising the encrypted first data set;

- fourth means for outputting the encrypted second data set for provision to another

5      party and for outputting the third data set for provision to the trusted authority.

The present invention also encompasses a computer program product for use in implementing the foregoing apparatus.

10

15

Brief Description of the Drawings

Embodiments of the invention will now be described, by way of non-limiting example, with reference to the accompanying diagrammatic drawings, in which:

. Figure 1      is a diagram illustrating the operation of a prior art encryption schema

20                   known as Identifier-Based Encryption;

. Figure 2      is a diagram illustrating how certain IBE operations are implemented by three different prior art IBE methods;

. Figure 3      is a diagram of an embodiment of the present invention; and

. Figure 4      is a diagram illustrating the flow of encryption and decryption

25                   operations performed by the Figure 3 embodiment.

Best Mode of Carrying Out the Invention

The Figure 3 embodiment of the invention concerns a computer system that allows a user to place an electronic order with a service provider where the service provider has

30      restricted access to the user's private and confidential information necessary to complete the order.

In particular, confidential information that is included in the order because it is required by the service provider to complete the transaction, for example the user's address, is encrypted with an IBE encryption key string; furthermore, this encryption key string is in itself an encrypted message from the user to the user's bank. The bank, acting as a trusted authority, is the only entity that is able to derive the IBE decryption key needed by the service provider to access the encrypted information included in the order. Accordingly, for the service provider to complete the transaction the service provider must provide the IBE encryption key string to the bank to allow the bank to derive the associated IBE decryption key. On receipt of the IBE encryption key string the bank decrypts it to access the message from the user (this message can, for example, include instructions to pay the service provider), while also providing the associated IBE decryption key to the service provider to allow the latter to decrypt the encrypted confidential information provided by the user to the service provider as part of the order.

More particularly, in Figure 3 there is shown a computer system 30 comprising a first computing entity 31, a second computing entity 32 and a third computing entity 33. Typically the three computing entities 31, 32, 33 are configured on separate computer platforms, however the computing entities 31, 32, 33 could be configured on a single computer platform. However the computing entities are configured, they are provide with suitable communication means for enabling them to inter-communicate; in the present example, the three computing entities 31, 32, 33 inter-communicate via the Internet 34. The communication between the various parties can make use of standard protocols such as HTTP and SOAP. Further, where required, secure connections can be established using secure protocols such as SSL.

Associated with the second computing entity 32 is a service provider 38 that offers goods and/or services on a website run by entity 32 and accessible via the network 34; as will be appreciated by a person skilled in the art, the service provider 38 could offer goods and/or services in a variety of ways, for example via email.

The first computing entity 31 is configured to allow a user 39 to access the service provider 38, via the second computing entity 32, to allow the user 39 to place an order with the service provider 38 for goods and/or service, as described below.

Associated with the third computing entity 33 is a bank 35 with which the user 39 has a bank and credit card account. The bank 35 is configured to act as a trusted authority. As depicted in Figure 4, the bank 35 makes publicly available certain information comprising:

- the public data 17 of an IBE method for which the bank performs the role of trusted authority – the corresponding private data is held by the bank 35;
- the public key 40 of a public/private key pair – the corresponding private key is held by the bank 35.

As will be appreciated by persons skilled in the art the trusted authority's public data 37 can be made available in a variety of ways, for example via a public web site (not shown).

Regarding the IBE method to which the public data 37 relates, in the following description of the Figure 3 embodiment, it will be assumed, by way of example, that the IBE algorithm being used is the QR algorithm described above with respect to Figure 1 with the user 39, service provider 38, and bank 35 respectively having the roles of the data provider 10, data recipient 11 and trusted authority 12. The public data 37 thus comprises the number $N$ formed from the bank's private data $p$ and $q$, and an indication of the hash algorithm $\#$ to be used.

The user 39 is provided with QR encryption software; this software is, for example, a software plug-in obtained from the bank's web site (not shown) and installed within the user's web browser (not shown). Preferably, the plug-in embeds knowledge regarding the bank's public data 37.

Similarly, the service provider 38 is provided with QR decryption software obtained from the bank 35 or from any other suitable source.

As regards the bank's public/private key pair (of which the public key is referenced 40), this could be a standard asymmetric key pair using a PKI infrastructure or another key pair such as one based on an IBE method.

The steps involved upon the user 39 placing an order with the service provider 38 will now be described.

Using the first computing entity 31 the user 39 downloads an order form 41 from the service provider 38 and completes the form for ordering specific goods and/or services (the completed form is referenced 42). The information used to complete the form may have different confidentiality categorisations, for example part of the order may be deemed non-confidential (such as goods and/or services required and associated quantities), while other parts of the order may be deemed to be confidential (such as the user's address required for delivery). Payment details for the order are not included on the order form but are included in a payment message 43 generated by the user 39 and intended for the attention of the user's bank 35; these payment details comprise, for example, the user's bank account number and the amount to be paid to the service provider 38.

Using the first computing entity 31 the user 39 now generates an IBE encryption key string (EKS) 44 to encrypt the completed order form 42 (or those portions of it categorised as confidential). The EKS 44 is generated (process 50) by encrypting the payment message 43 with the public key 40 associated with the bank 35, the resulting digital string of data bits being used to form, either alone or with other data, the EKS 44.

Once the encryption key string 44 has been derived, the completed form 42, or at least its confidential portions, are encrypted (process 51) using the described QR IBE

encryption method; the encryption parameters used for this encryption are the EKS 44 and the public data $N$ of the bank 35. The resultant form is herein called the encrypted form 45 regardless of whether it is all encrypted or is made up of a combination of plaintext and encrypted text.

5

The encrypted form 45, along with the encryption key string 44, is then sent to the service provider 38 by any suitable means, for example via e-mail or by being placed in a electronic public area.

10   In order for the service provider 38 to be able to decrypt the encrypted form 45, it must obtain a corresponding decryption key from the bank 35 acting in its role as the IBE trusted authority. To this end, the service provider 38 provides the EKS 44, as used by the user 39 to encrypt the completed order form, to the bank 45.

15   The bank uses the EKS 44, along with its private data, to generate the appropriate decryption key 47 (process 54). It may be noted that any change to the EKS by any party will result in a decryption key that will not decrypt the encrypted order form 45 correctly, thereby preventing the service provider 38 from understanding the order.

20   Additionally, the bank 35 uses its private key (corresponding to its public key 40) to decrypt the EKS 44 (process 53) thereby allowing the bank 35 to read the payment message created by the user 39.

In accordance with the user's instructions contained within the payment message the
25   bank 35 initiates payment to the service provider 38 for payment of the goods and/or services ordered by the user 39. At the same time, the bank 35 provides the decryption key 47 to the service provider 38 which uses it, along with the public data $N$ of the bank, to decrypt the encrypted order form 45 (process 46), or those portions that were encrypted, thereby recovering the completed order form 42 all in plaintext. The service
30   provider 38 thereafter fulfils the order upon receipt of payment from the bank.

The foregoing arrangement ensures that the user's payment message is inaccessible to the service provider 38 whilst ensuring that the payment message is passed on to the bank unchanged – if this is not done, then the service provider 38 is unable to read the order it has received from the user 39.

5

It will be appreciated that many variants are possible to the above-described embodiment. For example, the encryption key string 44 could comprise, in addition to the encrypted payment message, dynamic information such as a time component (for example, the time of payment message encryption) and/or a random number. The encrypted message used to form the encryption key string is not restricted to being a payment message and could be any sort of message though preferably it is a message with interpretable meaning – that is, not just a random string of bits as might be the case if a cryptographic key was being sent by the user to the trusted authority. Thus, for example, the message can be any sort of instruction to be interpreted and executed by the trusted authority. Alternatively or additionally, the message can be one or more conditions required to be satisfied by the service provider before the decryption key is generated and/or provided to the latter. One such condition could relate to the service provider being able to establish its identity to the satisfaction of the bank 35; another possible condition could relate to the date on which payment is to be made.

Rather than the message 43 intended for the bank 35 being encrypted using the public key 40 of a public/private key pair associated with the bank, it would be possible, though not preferred, for this message to be encrypted using a symmetric key known only to the user 39 and bank 35.

Instead of the QR IBE method, the above-described embodiment can be implemented using any other suitable algorithm, such as those mentioned above that use of Weil or Tate pairings, or are RSA based.

30

The computing entities 31 to 33 are typically based around program-controlled processors though specialized hardware can be provided for implementing at least some of the cryptographic functions described above.

5 The user 39 could provide the EKS 44 directly to the bank 35 as an alternative to, or in addition to, providing the EKS 44 to the service provider 38; in this case, additional information will typically also be provided to enable the service provider and bank to associate the EKS provided to the bank with the order provided to the service provider.

10